EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SMARTMATIC USA CORP.,
SMARTMATIC INTERNATIONAL
HOLDING B.V. and SGO
CORPORATION LIMITED,

Plaintiffs,

v.

MICHAEL J. LINDELL and MY
PILLOW, INC.,

Defendants.

Case No. 0:22-cv-00098-WMW-JFD

EXPERT DECLARATION OF BENJAMIN R. COTTON

September 22, 2023

I, Ben Cotton hereby declare and state as follows:

1) I am over the age of 18, and I understand and believe in the obligations of an oath. I make this declaration of my own free will and based on first-hand information and my own personal observations.

2) I am the founder of CyFIR, LLC (CyFIR).

3) I have a master's degree in information technology management from the University of Maryland University College. I have numerous technical certifications, including the Certified Information Systems Security Professional (CISSP), Microsoft Certified Professional (MCP), Network+, and Certified CyFIR Forensics and Incident Response Examiner.

4) I have over twenty-six (26) years of experience performing computer forensics and other digital systems analysis.

5) I have over nineteen (19) years of experience as an instructor of computer forensics and incident response. This experience includes thirteen (13) years of experience teaching students on the Guidance Software (now OpenText) EnCase Investigator and EnCase Enterprise software.

6) I have testified as an expert witness in state courts, federal courts and before the United States Congress.

7) I regularly lead engagements involving digital forensics and cyber security investigations for law firms, corporations, and government agencies. I am experienced with the digital acquisition of evidence under the Federal Rules of Evidence.

8) In the course of my duties, I have forensically examined voting systems in Maricopa County Arizona, Antrim County Michigan, Mesa County Colorado, Coffee County Georgia, and Adams Township, Michigan.

9) In the course of my duties, I have reviewed the administrative manuals and documentation for the Dominion Democracy Suite software and hardware components.

10) In the course of my duties, I have reviewed the administrative manuals and documentation for the Hart Intercivic software and hardware components.

11) In the course of preparing this declaration, I have reviewed the @SEC Source Code Review Report dated 2020-01-06 for the Los Angeles County VSAP system.

12) In the course of my duties, I have reviewed the Los Angeles County Voting System for All People (VSAP) certification 3.0 document set consisting of the following documents:

a) Los Angeles County VSAP 3.0 Admin Approval 8-22-2023 (PDF)

b) Los Angeles County VSAP 3.0 Approval (PDF)

c) Los Angeles County VSAP 3.0 Consultant's Accessibility Testing Report (PDF)

d) Los Angeles County VSAP 3.0 Consultant's Functional Test Report (PDF)

e) Los Angeles County VSAP 3.0 Consultant's Volume Test Report (PDF)

f) Los Angeles County VSAP 3.0 Consultant's Software Test Report (PDF)

g) Los Angeles County VSAP 3.0 Consultant's Security Test Report (PDF)

h) Los Angeles County VSAP 3.0 OVSTA Staff Report (PDF)

i) Los Angeles County VSAP 3.0 California Use Procedures (PDF)

13) In the course of my duties, I have reviewed the Los Angeles County Voting System for All People (VSAP) certification 3.0 document set consisting of the following documents:

a) County of Los Angeles VSAP 2.1 Certification October 1, 2020 (PDF)

b) County of Los Angeles VSAP 2.1 California Use Procedures (PDF)

c) County of Los Angeles VSAP 2.1 Executive Summary Report (PDF)

d) County of Los Angeles VSAP 2.1 Staff Report (PDF)

e) County of Los Angeles VSAP 2.1 Public Hearing Transcript (PDF)

f) County of Los Angeles VSAP 2.1 Consultant's Accessibility Testing Report (PDF)

g) County of Los Angeles VSAP 2.1 Consultant's Software Report (PDF)

h) County of Los Angeles VSAP 2.1 Consultant's Hardware Testing Report (PDF)

i) County of Los Angeles VSAP 2.1 Consultant's Security and Telecommunications Testing Report (PDF)

j) County of Los Angeles VSAP 2.1 Consultant's Functional Testing Report (PDF)

k) County of Los Angeles VSAP 2.1 Consultant's Volume Testing Report (PDF)

14) In the course of my duties, I have reviewed available public information from the Election Assistance Commission (EAC) regarding voting system certification status and the certification process for election software. In the course of this review, I determined that Smartmatic currently does not have any active certifications by the EAC for any of their voting systems.

15) A review of the @SEC Source Code Review Report dated 2020-01-06 highlighted a number of serious issues:

a) This report identifies the security vulnerabilities found through static code review and by searches of public vulnerability sources that could be exploited to alter vote recording, vote results, critical election data, such as audit logs, or to conduct a denial-of-service attack on the voting system.

b) There are a number of publicly known vulnerabilities that are present on the tested Smartmatic system. Specifically, "A search for public vulnerabilities was performed. Due to the high amount of third-party code, this activity returned a large number of publicly known vulnerabilities. Regardless of whether the vulnerabilities represent an actual risk to the voting system, the amount of code not controlled by the VSAP development team greatly increases the attack surface and the statistical likelihood of a problem in the future."

c) A static code analysis by @SEC revealed fourteen (14) low severity findings.

16) Based on my review of the @SEC Source Code Review Report dated 2020-01-06 the Smartmatic and VSAP devices have the following interfaces that are used for data transfer and communications with other networked devices:

a) USB ports

b) Ethernet Interfaces

c) Network Switches

d) The Election Central and Remote Voting sites use ethernet for network connectivity. These devices connect through an "air gapped" network.

e) Remote Voting is provided by Amazon Web Servers and is open to the public internet.

f) The devices have other wireless and Bluetooth capabilities that are reported to be disabled.

g) The report factors in compensating controls for detection of unauthorized access and time clock manipulation in the form of operating system log files that are not required to be preserved as an election record following an election.

h) The source code contains a significant number of source code files from third-party providers. These third-party source code files were not part of the scope of the evaluation and were not included in the analysis.

i) The cryptographic code on the VSAP is not running in a FIPS 140-2 approved environment as required. This fact results in non-compliance with the voting system requirements for the state of California.

j) The VSAP code contains hard coded passwords in the code.

k) No user lockout values are set for invalid password attempts, thus permitting unlimited password guesses and/or brute force password cracking attempts.

17) The Ballot Marking Device (BMD) utilizes a SQLLite database and the Tally utilizes Apache Cassandra.

18) The report revealed that there are over 290 vulnerabilities that exist in the VSAP system that could be leveraged independently and/or in combination to gain unauthorized or remote access to the VSAP system with sufficient privileges to modify the recorded votes within the system.

19) The SLI County of Los Angeles' VSAP Tally 2.1 Software Test Report for California that is posted on the California Secretary of State's VSAP web page as "County of Los Angeles VSAP 2.1 Consultant's Software Report (PDF)" is limited to the Tally 2.1 software and does not address the Smartmatic BMD testing or the testing of any other VSAP component[1].

20) I have reviewed the published Department of Homeland Security, Cyber Security & Infrastructure Security Agency (CISA) Best Practices for Securing Election Systems dated 11 November 2022 and last reviewed on 21 September 2023. Publicly available, this document can be located at https://www.cisa.gov/tips/st19-002. This document provides recommendations for securing election systems in the following areas:

a) Software and Patch Management – Note: The Analyzed Election Systems do not Comply with CISA Recommendations

b) Log Management - Note: The Analyzed Election Systems do not Comply with CISA Recommendations

c) Network Segmentation - Note: The Analyzed Election Systems Partially Comply with CISA Recommendations

[1] Los Angeles County VSAP: California Secretary of State

d) Block Suspicious Activity - Note: The Analyzed Election Systems do not Comply with CISA Recommendations

e) Credential Management - Note: The Analyzed Election Systems do not Comply with CISA Recommendations

f) Baseline Establishment for Host and Network Activity - Note: The Analyzed Election Systems do not Comply with CISA Recommendations

g) Organization-Wide IT Guidance and Policies – Note: The Analyzed Election Systems Comply with CISA Recommendations

h) Notice and Consent Banners for Computer Systems – Note: The Analyzed Election Systems Comply with CISA Recommendations

21) Based on my reviews of these documents, my cyber security experience, and my forensic analysis and my knowledge voting systems experience I find the following specific to the cyber security vulnerabilities and weaknesses observed in the voting systems of multiple vendors:

a) **<u>Failure to Update Antivirus Protections</u>** - Based on my personal knowledge and experience, over one million (1,000,000) new computer viruses are released on a daily basis. It is imperative to the security of any computing system or enterprise that the antivirus definitions be updated on a weekly basis. There is a systemic issue with all of the voting systems that I have had the opportunity to examine. There was an antivirus program installed on each of the systems. None of the system's antivirus definitions had EVER been updated following the installation of the voting software. For a system that had been in operation for two years, that would mean that the virus protection was so out of date that the system would not have prevented over seven hundred thirty million (730,000,000) versions of malware from compromising the voting system. To date Los Angeles County and Smartmatic have not produced a VSAP system for analysis. I would need to examine a VSAP system to determine if this finding is directly applicable to the Los Angeles County voting systems.

b) **Failure to Patch and Maintain Operating System (OS) Security** - Based on my personal knowledge, the companies that develop operating system software such as Windows, Linux, and Apple release software that contains unknown remote access vulnerabilities. These vulnerabilities can be used to gain unauthorized access to the targeted systems. Microsoft, the developer of the Windows family of software used on the Dominion PC-based Voting systems, releases operating system patches on a weekly basis to correct previously unknown operating system vulnerabilities and to prevent the possibility of unauthorized access to these systems. Based on my analysis of the voting systems in Maricopa County Arizona, Antrim County Michigan, Mesa County Colorado, Coffee County Georgia, and Adams Township Michigan there exists a consistent failure of the responsible authorities to patch or fix the operating system vulnerabilities on the voting systems. Typically, the producers of the operating systems will issue a weekly system patch/update which fixes newly discovered vulnerabilities. None of the voting system operating systems that I have examined had ever been properly patched for known cyber security vulnerabilities. By way of example, the Maricopa County voting system had not been patched for over 19 months and was not protected against three thousand five hundred twelve (3,512) known vulnerabilities. This finding in Maricopa County has proven to be consistent with all voting systems that I have analyzed, regardless of system or vendor. To date Los Angeles County and Smartmatic have not produced a VSAP system for analysis.

I would need to examine a VSAP system to determine if this finding is directly applicable to the Los Angeles County voting systems.

c) **Failure to Properly Establish and Control Assess to Voting Systems** - Based on my review of the electronic voting systems from different jurisdictions and from different vendors it is apparent that there is a systemic problem with access controls to the voting systems. First, in all examinations of the voting systems that I have conducted, the passwords were identical for all user accounts on that unique system. Second, these passwords were never changed by the local officials following the installation of the software. These two deficiencies result in long-term shared password exposure for multiple elections. Furthermore, there does not appear to be any accountability or assignment of the accounts to a specific individual for specific time periods. This makes individual accountability for actions performed by the account during an election impossible. CISA and industry best practices recommend that each username and password combination be unique and that each username password combination be assigned to only one individual. When that individual departs the username should be disabled to prevent unauthorized access to the system. When a new user arrives or is assigned, a new username and password are created for that user. Furthermore, best practices dictate that each individual password should be changed every ninety (90) days. This practice was not followed on the systems that I have had an opportunity to examine. To date Los Angeles County and Smartmatic have not produced a VSAP system for analysis. I would need to examine a VSAP system to determine if this finding is directly applicable to the Los Angeles County voting systems.

d) **No Process Monitoring, Network Monitoring or Baseline Monitoring** – Based on my review of the electronic voting systems from different jurisdictions, none of the jurisdictions had the capability to actively monitor programs that were running on the computers, monitor network activity, or had a process to alert election officials if a deviation from an approved baseline occurred. To date Los Angeles County and Smartmatic have not produced a VSAP system for analysis. I would need to examine a VSAP system to determine if this finding is directly applicable to the Los Angeles County voting systems.

e) **Log Management** – Retaining and adequately securing logs from both network devices and local hosts is a critical component of cyber security. Not only does a robust log management program support the detection and monitoring of real-time security postures, but in the event of an audit or a cyber security event, these logs support triage and remediation of historical cybersecurity events. None of the election systems that I have examined have an independent log management program. An effective log management program should include the following capabilities:

i) **Centralized Log Management**: It is common for hackers to delete, modify and/or otherwise manipulate logs and other artifacts as an integrated element of an unauthorized attack. An effective log management program would establish a centralized log repository that is not located on the device that generates the logged event. This method allows for unlimited log retention time periods, assurance of log preservation, ensures the integrity of the logs, and establishes a data repository to aid in the detection of malicious behavior. None of the election systems that I have analyzed forwarded logs to a centralized log management server. To date Los Angeles County and Smartmatic have not produced a VSAP system for analysis. I would need to examine a VSAP system to determine if this finding is directly applicable to the Los Angeles County voting systems.

ii) Security Information and Event Management – A security information and event management tool is commonly referred to as a SIEM. I have personal experience with, and have observed, threat actors attempting to delete local logs to remove on-site evidence of their activities, including log deletion, log modification and changing logging settings. By sending logged events to a SIEM tool, an organization can reduce the likelihood of malicious log spoilation and maximize the ability to detect malicious activity. None of the election systems that I have analyzed utilized a SIEM. To date Los Angeles County and Smartmatic have not produced a VSAP system for analysis. I would need to examine a VSAP system to determine if this finding is directly applicable to the Los Angeles County voting systems.

iii) Effective log correlation from both network and host security devices is critical to protecting election networks and computing devices. By reviewing logs from multiple sources, an organization can better triage an individual event and determine its impact to the entire organization. Today’s modern log analysis and correlation systems will provide the analysis, detection of an anomaly, and alerting within 15 seconds from event to eyes on glass by an analyst. None of the election systems that I have analyzed were capable of log correlation. To date Los Angeles County and Smartmatic have not produced a VSAP system for analysis. I would need to examine a VSAP system to determine if this finding is directly applicable to the Los Angeles County voting systems.

iv) Review both centralized and local log management policies to maximize efficiency and retain historical data. CISA recommends that organizations retain critical logs for a minimum of one year, if possible. Federal law requires that all election system-related logs be retained for at least 22 months. In practice many jurisdictions are not preserving the operating system logs as part of that election data retention. This is problematic in the case of Los Angeles County as a reliance on the operating system logs is relied upon as a compensating control to detect unauthorized access, data manipulation and date/time manipulation[2]. To date Los Angeles County and Smartmatic have not produced a VSAP system for analysis. I would need to examine a VSAP system to determine if this finding is directly applicable to the Los Angeles County voting systems.

v) PowerShell and Advanced Logging Should be Enabled.

(1) PowerShell is a cross-platform command-line shell and scripting language that has quickly become a central exploitation capability by malicious actors. I have personally observed threat actors, including advanced persistent threat (APT) actors, using PowerShell to exploit systems and hide their malicious activities. To date Los Angeles County and Smartmatic have not produced a VSAP system for

[2] ATSEC Source Code Review Report VSAP Version 2.0 dated 01.06.2020.

analysis. I would need to examine a VSAP system to determine if this finding is directly applicable to the Los Angeles County voting systems.

(2) Given the extensive usage of Powershell to exploit systems by malicious actors, it is imperative that the PowerShell instances have module, script block, and transcription logging enabled. To date Los Angeles County and Smartmatic have not produced a VSAP system for analysis. I would need to examine a VSAP system to determine if this finding is directly applicable to the Los Angeles County voting systems.

f) **Network Segmentation** – In all the election systems that I have examined there has been an attempt to segment the systems that record the votes from the systems that administratively support the voting process, (e.g. poll worker laptops, voter registration data base, etc.). The only form of segmentation however is to use an "air gap" to attempt to isolate the voting systems from the public internet. This partially complies with the CISA Best Practices for Securing Election Systems. The issue is the over reliance on the manner in which the air gap is implemented and the false security that, because there is no stated connections to the internet, there can be no connection to the internet or breaching of that "air gap". History has proven that air gaped systems are easily defeated by connecting cell phones, wireless "hockey pucks", and other wireless networks to an endpoint internal to the air gapped systems. It is important to note that all of the computers used within each voting system that I have examined are commercial off-the-shelf (COTS) hardware. Based on my review of the Los Angeles County documentation this appears to be the case with the VSAP as well. Depending on the configuration of the wireless device modems contained on the mother boards of the COTS equipment, simply creating a nonpassword protected WiFi network that is in range of a device is sufficient for that device to automatically connect to the internet. An analysis of the systems that I have had the opportunity to physically examine have revealed that these COTS systems do contain built in wireless 802.11 and cellular modems that can connect to unauthorized networks if the user has administrative access, even if the design of the network was purportedly air gapped. Given the number of vulnerabilities that were discovered as part of Los Angeles' own testing, such administrative access is not anticipated to be difficult on the VSAP system. It should be noted, however, that remote access, code modification and system modification can be executed on air gapped systems through the use of USB devices, direct communication with exterior devices are not required. STUXNET and the Chinese APT31 are examples of this type of compromise[3]. Given the presence of USB ports and the procedures for using USB devices, the VSAP would be susceptible to this type of attack. Based on the VSAP documentation that I have reviewed, however, it is clear that all the components of the VSAP system are networked.

g) **The BMG Network is not Truly Air Gapped -** The documentation for the VSAP system indicates that this is an "air gapped" system. This assertion stands in contrast to the inclusion of the remote voting sites as part of that network and the documented statements that at least a portion of the remote voting sites exist in the Amazon Cloud. The term "air gap", in general security usage, means that there are a number of components on one physical site that are connected via ethernet connections and that there are no connections to establish a link outside of that one physical location. The term "remote voting sites" as

[3] https://thehackernews.com/2023/08/chinas-apt31-suspected-in-attacks-on.html

part of the network diagram and discussion indicates that these sites are not collocated with the centralized voting system and furthermore the @TEC Source Code Review document implicitly states that the remote voting sites are connected by ethernet and exist in the Amazon Cloud. I have found no indication that all of the remote voting locations have been supplied with a dedicated direct ethernet cable which runs from the location of the central voting system and the remote voting site, and I have personal knowledge that the Amazon Cloud is only accessible via the public internet. Therefore, the fact that remote voting sites are part of the network means, by definition, that the communications to those remote sites are transported by public internet and/or commercial communications networks. That would make the voting system communications susceptible to interception and possible manipulation even if that communication is tunneled through a virtual private network (VPN) or other medium. To date Los Angeles County and Smartmatic have not produced a VSAP system for analysis. I would need to examine a VSAP system to determine if this finding is directly applicable to the Los Angeles County voting systems.

h) **Block Suspicious Activity** – In every election system that I have analyzed there has been no mechanism for blocking malicious activity or programs other than the outdated antivirus program. Given the lack of operating system patching, lack of antivirus definition updating, the lack of user/password controls, and the extreme amount of system vulnerabilities, these systems simply do not have the ability to detect or block suspicious activity from a current threat actor. To date Los Angeles County and Smartmatic have not produced a VSAP system for analysis. I would need to examine a VSAP system to determine if this finding is directly applicable to the Los Angeles County voting systems.

22) Given the totality of the lack of practical, effective cybersecurity protections on all of the election systems that I have examined, coupled with the lack of effective access controls to the systems, it is a near certainty that the VSAP systems would be vulnerable to unauthorized access and vote manipulation through technical processes. To date Los Angeles County and Smartmatic have not produced a VSAP system for analysis. I understand that Smartmatic has recently acknowledged that it has an exemplar BMD machine that it has not provided to Defendants' counsel. Once I receive this machine, I will be able to supplement my report. I would need to examine a VSAP system to definitely prove if this finding is directly applicable to the Los Angeles County voting systems.

I declare under penalty of perjury under the laws of the United Sates of America that the foregoing is true and correct.

Executed on 22 September 2023

Benjamin R. Cotton

BENJAMIN R. COTTON

27427 Montana Hwy 83
Bigfork, MT 59911

Office Phone: (703) 659-9805
Email: bencotton@cytechservices.com

CAREER SUMMARY

A technical and managerial professional with over 20 years of experience in Computer Forensics and Cyber Security, Mr. Cotton has worked in both commercial industry and in the Federal Government. Mr. Cotton has served as a subject mater expert on the forensic software "Encase", teaching as a part-time instructor for Guidance Software. He holds an active Top Secret/SCI clearance with lifestyle polygraph. His Computer Forensics experience was gained in both the laboratory and the field, and he is trained to the highest Federal law enforcement standards. Mr. Cotton also serves on the Cyber Security Advisory Board for Brigham Young University.

EDUCATION

May 2002	*Master of Science Degree*, Information Systems Management University of Maryland

PROFESSIONAL CERTIFICATIONS

- Drug Enforcement Administration Computer Forensic Examiner
- Certified Information Systems Security Professional (CISSP)
- Networks Plus (Net+)
- Microsoft Certified Professional (MCP)
- CyFIR Certified Examiner

EMPLOYMENT

eSentire, USA.
Contracted to United States Government and Commercial Clients
June 2021 – Present
Vice President of Incident Response

- Serves as the Vice President in charge of the Incident Response functions of eSentire.
- Serves as a Subject Matter Expert on CyFIR and cyber security.
- Serves as a Subject Matter Expert senior instructor in the use of the AIX/CyFIR enterprise forensic software.
- Serves as a Subject Mater Expert to DHS HIRT Surge
- Perform computer forensic examinations in support of the United States Government and commercial clients, specializing in incident response, law enforcement, counter-terrorism and information operations cases.
- Testifies as required in Federal, State and Local proceedings concerning case findings.
- Expert in multiple forensic software tools including CyFIR, EnCase, FTK, ILook, SMART, WinHEX, Quincy, Cellubrite, XRY, Oxygen Detective, Paraben Device Seizure, R-Studio, Red Hat Linux utilities and over 150 supporting specialty forensics and security programs..
- Prepares reports of findings for dissemination to multi-level audiences.
- Interfaces with clients in support of cases and examinations.
- Provides formal and informal training on a variety of computer forensic topics, both domestically and internationally.
- Prepares reports of findings and case testimony.
- Performs research and development in the field of Computer Forensics.
- Mentors and coaches new examiners in both technical and corporate areas.
- Creates customized scripts and programs to facilitate efficient computer forensic examinations.

CyTech/CyFIR, Inc.
Contracted to United States Government and Commercial Clients
July 2007 – June 2021
Founder/Senior Computer Forensic Examiner

- Serves as the President and CEO of the company.
- Serves as a Subject Matter Expert on CyFIR and cyber security.
- Served as a contract instructor for Guidance Software, teaching EnCase at all levels from entry level to advanced subjects.
- Serve as a senior instructor in the use of the CyTech Forensic and Incident Response (CyFIR) enterprise forensic software.
- Perform computer forensic examinations in support of the United States Government and commercial clients, specializing in incident response, law enforcement, counter-terrorism and information operations cases.
- Testify as required in Federal, State and Local proceedings concerning case findings.
- Expert in multiple forensic software tools including CyFIR, EnCase, FTK, ILook, SMART, WinHEX, Quincy, Cellubrite, XRY, Oxygen Detective, Paraben Device Seizure, R-Studio, Red Hat Linux utilities and over 150 supporting specialty forensics and security programs..
- Prepare reports of findings for dissemination to multi-level audiences.
- Interface with clients in support of cases and examinations.
- Perform research and development in the field of Computer Forensics.
- Design of new hardware and software platforms to improve examiner efficiency and group knowledge sharing.
- Provide formal and informal training on a variety of computer forensic topics, both domestically and internationally.
- Prepare reports of findings and case testimony.
- Perform research and development in the field of Computer Forensics.
- Create training programs and provided training for fellow examiners in aspects of computer forensics and digital evidence. These programs are presented both domestically and internationally.
- Mentor and coach new examiners in both technical and corporate areas.
- Trained and skilled in conducting examinations in accordance with established Department of Justice rules of evidence and chain of custody.
- Designed and implemented advanced systems for processing digital evidence and forensic investigations.
- Developed and implemented Standard Operating Procedures to ensure future ASCLAD certification.
- Create customized scripts and programs to facilitate efficient computer forensic examinations.
- Discovered, investigated and remediated the largest breach in U.S. Government History (OPM).

ETG, Inc.
Contracted to the United States Government and Civilian Clients
Sep 2003 – July 2007
Director / Senior Computer Forensic Examiner

- Served as the Director, Commercial Litigation Support Division
- Managed an on-site team of Computer Forensic Examiners.
- Performed computer forensic examinations in support of the United States Government and commercial clients, specializing in counter-terrorism and information operations cases.
- Utilizes multiple software tools including EnCase, FTK, ILook, SMART, Quincy, and Red Hat Linux utilities.
- Prepared reports of findings for dissemination to multi-level audiences.
- Interfaced with customers in support of cases and examinations.
- Performed research and development in the field of Computer Forensics.
- Assisted in the design of new hardware and software platforms to improve examiner efficiency and group knowledge sharing.
- Provided formal and informal training on a variety of computer forensic topics.

Computer Sciences Corporation
Contracted to the United States Drug Enforcement Administration
April 2003– Sep 2003
Senior Computer Forensic Scientist

- Performed computer forensic acquisitions and examinations in support of Drug Enforcement Administration (DEA) cases on numerous hardware and software platforms.
- Performed in-depth forensic analysis using multiple tools including ILook 7, EnCase 3 & 4, SMART, and Red Hat Linux utilities.
- Performed on-site searches and assists in the seizure of digital evidence related to drug-based investigations.
- Prepared reports of findings and case testimony.
- Interfaced with DEA agents and support staff in support of DEA cases.
- Performed research and development in the field of Computer Forensics.
- Created training programs and provided training for fellow examiners in aspects of computer forensics and digital evidence.
- Mentored and coached new CSC examiners in both technical and corporate areas.
- Skilled with the Encase, Paraben, Forensics Toolkit, Ilook, and Smart forensic tools, as well as over 150 supporting specialty exploitation programs.
- Trained and skilled in conducting examinations in accordance with established Department of Justice rules of evidence and chain of custody.
- Designed and implemented advanced systems for processing digital evidence and forensic investigations.
- Developed and implemented Standard Operating Procedures to ensure ASCLAD certification.
- Served as a subject matter expert to US Attorney's in support of prosecutions.
- Created customized scripts and programs to facilitate efficient computer forensic examinations.
- Served as a part-time Guidance Software instructor for the Encase software.

United States Army
Special Operations Command
May 1997 – April 2003
Special Forces Warrant Officer

- Commanded a 7 man computer forensic detachment.
- Designed and implemented a deployable computer forensics capability for the command, using Encase, Forensic Toolkit, SMART, and Ilook programs for the core forensic examination capability.
- Conducted computer forensic operations in support of the Global War on Terrorism and National Level Directives.
- Prepared reports and follow-on targeting information for dissemination to tactical and strategic units based on findings from computer forensic operations.
- Developed Computer Security Tactics, Techniques and Procedures (TTP) to ensure computer operational security. Used computer forensic techniques to evaluate TTP's and to recommend operational changes in computer usage.
- Interfaced with theater level combatant commands to ensure integration and execution of computer forensic operations.

Guidance Software

April 2003 – April 2014
Contracted Instructor

- Instruct students in all aspects of the Encase Computer Forensic Software.
- Assist in developing and reviewing the program of instruction (POI) for Encase Forensic, Enterprise and e-Discovery software
- Act as an initial tester of new release software

CLEARANCE INFORMATION

- Current TS/SCI clearance with lifestyle polygraph examination

PROFESSIONAL MEMBERSHIPS

- Member, International Association of Computer Investigative Specialists (IACIS)
- Institute of Computer Forensic Professionals
- Member of Cyber Security Advisory Board, Brigham Young University

NOTABLE FORENSIC AND INCIDENT RESPONSE ACCOMPLISHMENTS

- Lead forensic examiner in the Banco Progreso vs. Pedro Castillo matter. This engagement started with three laptops and turned into the largest individual bank fraud case in the history of the International Monetary Fund. Banco Progreso ultimately was able to recover over $100M in stolen funds.
- Lead forensic examiner in the Lockheed Martin vs. L-3 Communications lawsuit over the ATARS contract. This investigation led to a $3.2B settlement for my client.
- Discovered the Office of Personnel Management Breach. This breach was the largest breach in the history of the US Government and had been present in US Government networks for almost three years prior to my involvement and discovery.
- Designated as an on call subject matter expert (SME) to the Department of Homeland Security (DHS) hunting and incident response teams (HIRT).

ADDITIONAL COURSES AND SEMINARS

- DHS BIRT 2022
- Splunk Cybersecurity 2021
- Memory Forensics, Volatility 2016
- Techno Security 2015
- Gartner, 2014
- RSA, 2014
- Cyber Security Innovation Forum 2014
- CIO Security Conference, 2013
- PFIC 2009, 2011, 2013
- CEIC 2008
- Techno Forensics 2007, 2009, 2011,2013
- Techno Security, 2007, 2010, 2013
- HTCIA International Conference and Symposium 2006
- HTCIA International Conference and Symposium 2004
- EnCase Advanced Computer Forensics Course, Guidance Software
- MCSE (Windows 2000), 2003
- Unix System Administrator, 1996
- Ultimate Hacking Course, 2001
- Encase Field Intelligence Module (FIM), Guidance Software, 2005, 2006, 2008, 2012 *
- Encase Internet Email Investigations, Guidance Software 2003, 2006, 2009, 2011, 2013 *
- Encase Advanced Course – NTFS, Guidance Software 2004, 2011, 2013 *
- Encase Intermediate Course, Guidance Software 2001, 2007, 2010, 2013*
- Encase Basic Course, Guidance Software 2000, 2010, 2011 *
- ILook Computer Forensic Analysis In-Service Training Course, DEA 2003
- Computer Forensic Examiner Training, DEA Digital Evidence Laboratory, 2003
- CISSP, 2003
- MSP, 2003

* Indicates courses that I taught for Guidance Software

TECHNICAL SKILLS (PARTIAL LIST)

- CyFIR – Expert Level
- Encase – Expert Level
- Enscripting Program Language (Expert Experience)

- Microsoft Windows 10, 7, Vista, XP, 2000, NT, 98, 95, 3.1, Server 2012, Server 2016, Server 2019 and DOS Operating Systems *(Strong Experience)*
- Macintosh OS X *(Strong Experience)*, Macintosh System 9 and lower *(Moderate Experience)*
- Linux *(Moderate Experience)*
- UNIX and Be operating systems *(Strong Experience)*
- Ios, Android, Pocket PC (Windows CE) and Palm OS handheld devices *(Strong Experience)*
- Computer forensic software utilities such as CyFIR, X-Ways, Axiom, EnCase, SMART, Red Hat Linux utilities, Oxygen Forensics, , and associated forensic hardware tools *(Expert Experience)*
- Memory Forensics, Volatility, Redline, and CyFIR (Strong Experience)
- Oracle, Microsoft SQL Server, and Microsoft Access databases *(Strong Experience)*
- Expert knowledge of numerous governmental, commercial, and consumer level application software packages in both the Windows and Macintosh environments
- Bilingual in Spanish with a DLPT of 3/3

Speaking Engagements

- Net Diligence
  Incident Response
  Philadelphia, PA 2022
- Net Diligence
  Incident Response
  Ft. Lauderdale, FL 2022
- Enterprise Forensics
  Investor Conference
  Virtual, 2020
- Incident Response at Enterprise Scale
  CAN Conference
  Virtual, 2020
- CISO Conference
  Forensic Preparedness
  Virtual, 2020
- Enterprise Forensics and IR
  Imperial Capital Investors Conference
  New York, NY 2019
- Digital Forensics Workshop
  Tampa, FL 2019
- When Forensics Gets In the Way
  Washington, DC 2019
- NASDAQ Incident Response Panel
  New York, NY 2019
- NASDAQ Cyber Security Summit
  New York, NY 2018
- US Embassy Cyber Summit
  Computer Forensics and Cyber Security
  Athens, Greece, 2018
- Block Chain Summit, 2018
  Computer Forensics and Cyber Security
  Carnegie Mellon University
  Pittsburgh, PA
- Information to Intelligence (I2i) Summit, 2018
  Endpoint Data Exploitation
  Denver, CO
- Net Diligence Cyber Risk Summit, 2018
  Endpoint Visibility
  Philadelphia, NJ 2018
- CIO Summit, 2017
  Austin, TX
  Topic: Endpoint Forensics and Visibility

– Pittsburgh Association for Financial Professionals, 2017
Pittsburgh, PA
Topic: Incident Response/Breach Panel
– Cyber Risk Management Conference
Toronto, Canada
Topic: Cyber Security
– BPIC Conference
Palm Beach, FL
Topic: Securing the Internet of Things (IoC)
– Alabama Trial Lawyers Association, 2017
Montgomery, AL
Topic: Digital Forensics
– Wyoming Trial Lawyers, 2016
Cheyenne, Wy
Topic: Digital Forensics
– Techno Security, 2016
Myrtle Beach, SC
Topic: Enterprise Digital Forensics
– 36th Annual Association for Governmental Leasing and Finance (AGLF) Conference, 2016
Las Vegas, NV
Topic: Cyber Security
– ISSA LA May Healthcare Privacy & Security Forum, 2016
Los Angeles, CA
Topic: Detection of Zero Day Malware
– Pittsburgh Association for Financial Professionals, 2016
Pittsburgh, PA
Topic: Incident Response/Breach Panel
– SouthernCal Edison Conference 2016
Los Angeles, CA
Topic: Protecting the Power Grid IoC
– Kasperski Analyst Conference, 2016
Tenerife, Spain
Topic: Incident Response
– North America Cyber Summit, 2015
Detroit, MI
Topic: Advanced Cyber Security and Assessments
– Cyber Security Panel 2015
Deer Valley, UT
Topic: Cyber Security
– Techno Security Conference 2015
Myrtle Beach, SC
Topic: Advanced Cyber Security
– MAPI Cyber Security Forum 2014
Pittsburgh, PA
Subject: Cyber Forensics and Incident Response
– Cyber Security Innovation Forum 2014
Baltimore, MD
Subject: Incident Response and Network Forensics
– CIO Security Conference, 2013
Austin, TX 2013
Subject: Digital Forensics and Incident Response in the Enterprise
– PFIC 2013
Salt Lake City, UT
Subject: Networked Forensics
– International Cyber Security Panel, 2013
Washington, DC
Responding to Cyber Threats on a Global Scale
– Techno Security Conference, 2011

Myrtle Beach, SC
Topic: Volatile Memory Forensics

- October 29, 2007
  Techno Forensics Conference
  Gaithersburg, MD
  Topic: E-Discovery and Computer Forensics
- July 16, 2007
  Annual ACFE Conference and Exhibit
  Orlando, FL
  Topic: Cell Phone Forensics
- June 3-6, 2007
  Ninth Annual Techno Security Conference
  Myrtle Beach, SC
  Topics: P2 Enterprise Forensics, Laboratory Practicals and E-Discovery: The New Frontier.

Expert Witness Testimony

- Sworn statements and expert witness testimony Bockbank v. Tenold, Ravali District Court, June 2023, Montana
- Multiple sworn statements and expert witness testimony Kari Lake v. Kathleen Hobbs et al 2022, Arizona
- Multiple Sworn Declarations – Baily v. Antrim County Michigan 2021-2022
- Sworn statements and expert witness testimony State of Wyoming v. Kreusel October 2021, District Court, Sweetwater County, Wyoming
- Multiple Testimony Appearances before the Arizona State Senate, June 2021 to September 2021
- 14 October 2021, Wyoming v. Kreusel, District Court18 May 2015, Pope v. Davis, Circuit Court, Gillette, Wyoming
- Testimony to the US House of Representatives Committee on Oversight and Government Reform, OPM Breach, multiple times, June 2015 to September 2015, Washington, DC
- Multiple Sworn Declarations, Dec 2014 to May 2015, Nike v. Adidas, Portland, OR
- Multiple Sworn Declarations, Feb 2015 to July 2015, Nike v. Under Armour, Portland, OR
- 18 June 2008, Banco Progresso v. Pedro Castillo, 11th Judicial Circuit, Miami, FL
- 31 October 2007, Lockheed Martin v Speed, Fleming, St. Romain et al, Deposition Locaton: Ford and Harrison Office, Orlando, FL
- July 2006, DAG Petroleum v. BP Petroleum, Deposition Location: Washington, DC
- 19 February, 2009, Tacaronte v. Lesinski, Deposition Location: Virginia Beach, VA
- 9 December 2010, Wyoming v. Mersereau, Location: Douglas, Wyoming
- Multiple sworn statements and affidavits 2015-2023 in other matters

Ben Cotton
27427 Montana HWY 83
Bigfork, MT 59911

Fee Schedule

Litigation: $350.00 per hour for services including, but not limited to, review, research and analysis: reports, conferences, site visitation and survey where appropriate together with a review of all Discovery materials and any other materials deemed necessary to reach and render an opinion in the subject litigation.

Deposition: Deposition fee will be $450.00 per hour with $1000.00 minimum to be pre paid by opposing counsel on or before the date of deposition.

Trial: $450.00 per hour with $1250.00 minimum.

Cancellation: Counsel is required to provide forty-eight (48) hour notice of cancellation of scheduled deposition or testimony or be subject to a four (4) hour cancellation fee plus any travel expenses.

Travel: Travel time is billed at $350.00 per hour. Client is responsible for all actual travel expenses (travel, lodging, meals etc)

Invoices: All invoices are due and payable within 15 (15) days of receipt. Invoices thirty (30) days past due will be charged interest at the rate of 1.5% per month (annual rate of 18%), and will be assessed a $200.00 late fee. Invoices sixty (60) days past due will be referred for collection and all legal remedies for payment pursued.

Payment: The attorney/attorney firm is solely responsible for fee payment.